Information Warfare
and
Cyber Defense

Mr. Larry Wright
Booz Allen Hamilton

April 2002
<table>
<thead>
<tr>
<th>1. REPORT DATE (DD-MM-YYYY)</th>
<th>2. REPORT TYPE</th>
<th>3. DATES COVERED (FROM - TO)</th>
</tr>
</thead>
<tbody>
<tr>
<td>22-04-2002</td>
<td>Briefing</td>
<td>xx-xx-2002 to xx-xx-2002</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4. TITLE AND SUBTITLE</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Warfare and Cyber Defense</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5a. CONTRACT NUMBER</th>
<th>5b. GRANT NUMBER</th>
<th>5c. PROGRAM ELEMENT NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5d. PROJECT NUMBER</th>
<th>5e. TASK NUMBER</th>
<th>5f. WORK UNIT NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6. AUTHOR(S)</th>
<th>7. PERFORMING ORGANIZATION NAME AND ADDRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wright, Larry ;</td>
<td>Booz Allen Hamilton</td>
</tr>
<tr>
<td></td>
<td>8283 Greensboro Drive</td>
</tr>
<tr>
<td></td>
<td>McLean, VA 22102</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>8. PERFORMING ORGANIZATION REPORT NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS</th>
<th>10. SPONSOR/MONITOR’S ACRONYM(S)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Booz Allen Hamilton</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>11. SPONSOR/MONITOR’S REPORT NUMBER(S)</th>
<th>12. DISTRIBUTION/AVAILABILITY STATEMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>APUBLIC RELEASE</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>13. SUPPLEMENTARY NOTES</th>
<th>14. ABSTRACT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>See report.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>15. SUBJECT TERMS</th>
<th>16. SECURITY CLASSIFICATION OF:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>a. REPORT</td>
</tr>
<tr>
<td></td>
<td>Unclassified</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>17. LIMITATION OF ABSTRACT</th>
<th>18. NUMBER OF PAGES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Release</td>
<td>46</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>19. NAME OF RESPONSIBLE PERSON</th>
<th>19b. TELEPHONE NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>email from Booz Allen (IATAC), (blank)</td>
<td>International Area Code</td>
</tr>
<tr>
<td><a href="mailto:llfenster@ditc.mil">llfenster@ditc.mil</a></td>
<td>703767-9007</td>
</tr>
<tr>
<td></td>
<td>DSN 427-9007</td>
</tr>
</tbody>
</table>

Standard Form 298 (Rev. 8-98)  
Prescribed by ANSI Std Z39.18
**Title and Subtitle:** Information Warfare and Cyber Defense

**Author(s):** Wright, Larry

**Performing Organization:**
Booz Allen & Hamilton
8283 Greensboro Drive
McLean, VA 22102

**Sponsoring/monitoring Agency:**
Booz Allen Hamilton

**Abstract:**
Briefing about information warfare from the Phoenix Challenge 2002 Conference and Warfighter day.

**Subject Terms:**
IATAC Collection, information warfare, information assurance, cyber warfare

**Numbers and Code:**
- **Number of Pages:** 45
- **Price Code:**
- **Distribution Code:** A

**Security Classification:**
- **Report:** UNCLASSIFIED
- **Page:** UNCLASSIFIED
- **Abstract:** UNCLASSIFIED

**Notes:**
Approved for public release; Distribution unlimited

**Form:**
Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18
298-102
• Massive networking has made the U.S. the world’s most vulnerable target for information attack

• Public and Private infrastructures have become virtually indistinguishable and largely global
USG/DoD is highly dependent on civilian infrastructure, and shared capability = shared vulnerability
Information Technology Trends

Power Is Up

(Source: EIA, CNET, Gartner, Dell -- 2000)
Information Technology Trends

Price Is Down

Cost per MIPS*

* Millions of Instructions Per Second

(Source: Business Week, Jan -- 2002)
Attacks Are Growing Significantly

Commercial & DoD Incident Reports

- Commercial
- DoD

Year: 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 00, 02
Increasing Vulnerabilities

- Number of Intrusions
- Denial of Service Attacks
- Velocity and Damage of Viruses
- Other Nations’, Terrorists’, and Criminals’ sophisticated cyber attack capabilities

“...30 computer virtuosos strategically located around the world, with a budget of less than $10 million, could bring the U.S. to its knees.”

-- Center for Strategic and International Studies (CSIS)
Virus Attacks: Accelerating in Speed & Damage

Sources: ICSA.net, Carnegie Mellon CERT

- **“Jerusalem” Virus**: 3 years - $50M Damage
- **“Concept” Virus**: 4 Months - $50M Damage
- **“Code Red” Worm**: 9 Hours ~ $2.6 B Damage
- **“Sircam” Worm**: 6 Hours ~ $1.3B
- **“Love Bug”**: 5 Hours - >$800M Damage
- **“Melissa” Virus**: 4 Days ~ $300M Damage

Time to Become Most Prevalent Virus

1990 1995 2000
Findings:

- Many agencies have no meaningful system to test or monitor system activity or detect intrusions.
- General lack of policy or programs to detect, report, or share information on vulnerabilities or attacks.
- Most employees lack basic awareness or education on computer security.
- Few agencies ensure contractor compliance on security requirements or background checks.

In last year’s penetration testing, nearly all Federal agencies earned a grade of “D” or lower for computer security – DoD earned the only passing grade.
Information
Operations
Information Superiority

Range of Operations

IO
IW
C2W

Levels of War

Peace  Crisis  Conflict/War  War Termination  Peace

Operational

Strategic

Tactical
### Knowledge and Interest Are Widespread

**IA / IO / IW**

**A 10-Day Sample**

<table>
<thead>
<tr>
<th></th>
<th>E-mail</th>
<th>Links</th>
<th>Articles</th>
<th>Web Sites</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IA</strong></td>
<td>38</td>
<td>32</td>
<td>23</td>
<td>2350</td>
</tr>
<tr>
<td><strong>IO</strong></td>
<td>22</td>
<td>16</td>
<td>8</td>
<td>2713</td>
</tr>
<tr>
<td><strong>IW</strong></td>
<td>7</td>
<td>11</td>
<td>2</td>
<td>26</td>
</tr>
</tbody>
</table>

| Related Subjects | 16 | 34 |
| Conferences      | 5  | 5  |

January 2002
IO “Threat” is Very Non-Traditional

- The IO “Threat” aims to diminish or destroy DoD’s capability to gain and maintain Information Superiority

- Examples include:
  - Trusted insider who takes advantage of access
  - Insertion of malicious code into our system
  - Modification of our hardware or software, including possibly at the supplier level
  - Remote “virtual” attack
  - Empowered “virtual” agents
  - New approaches that have not yet been discovered

- Murphy’s law, natural events, and system fragility all exacerbate likely problems

- Commercial sector will not meet all USG/DoD security needs
The Insider Threat

Source: GartnerGroup Report 5605
• Today’s primary spending is on high likelihood threats, but their impact is low

• A much lesser amount is spent on low likelihood threats that will have a high impact
Today...

- Broadly based, fairly uncoordinated USG/DoD efforts are underway.
- Public awareness of IW and IA issues at home and abroad is dramatically greater.
- Internet use has exploded and USG/DoD use and dependence on the internet has grown exponentially.
- We have an increased appreciation of our vulnerabilities from IW.
- Remediation and preparations for Y2K diverted focus and potential funds from IA/IW resolution.
- A tremendous amount of energy is ongoing nationally, which is likely - over time - to substantially improve U.S. IA/IW capabilities.
- A combined WMD/IW attack could be potentially devastating.
The 1993 World Trade Center bombing appeared to be a traditional Terrorist attack -- significant because of its size and planning on U.S. soil.

In fact: The Terrorists intent was to topple the towers on Wall Street inciting a crisis in U.S. financial markets.

Therefore, “intent” to impact/degrade/destroy the U.S. Economy has been demonstrated.

How long until there is a Cyber-terrorism event with the same intent?
The 9-11 World Trade Center attack went well beyond a traditional Terrorist attack -- The long term planning and coordination on U.S. soil coupled with the attack on the Pentagon made this an act of war.

In fact: The Terrorists intent was to incite a crisis in U.S. financial markets and demonstrate U.S. inability to protect itself.

Once again, “intent” to impact/degrade/destroy U.S. infrastructure was clearly demonstrated.

How much worse would 9-11 have been if it included a Cyber-terrorism element with the same intent?
Our National Security Posture
Our concept of national security has always pivoted around the physical and economic well-being of the American people.

For 200 years, this protection has largely been achieved beyond US shores.

Today, defense of our economics and people must take place on US soil too!

Threats may now even be “remote” -- attacks against the US proper, from beyond our shores.

In the Information Age, our wealth, security, and functionality are all rooted in our ability to control information.

National security can no longer isolate the role of DoD and the Intelligence Community from the business and private sector.

Our national security must now become the responsibility of the United States -- Not simply the Defense Department!
We Are A Nation At Risk

• Today, in the Information Age, we are the most vulnerable:
  – Each of our infrastructures is dependent on others
  – Globalization and financial integration is pervasive
  – We must protect everywhere from attacks anywhere
• The conflict is engaged: Solar Sunrise, Moonlight Maze, Melissa, Love Bug, Denial of Service, Code Red, Sircam
• The “nuclear threat” now is widely available to almost any nation or group as WMD or Information Warfare technologies
  – Consider information as a weapon of mass effect (WME)
• NSA conducted a significant number or Red Team exercises during the last five years, using tools and techniques downloaded from the Internet
  – 99% of attacks undetected

We are awaiting a “Cyber Pearl Harbor,” when we are already involved in a “Battle of Britain”
So What?

- Our concept of national security must adapt to this changing world. In fact, a new concept already is emerging. It encompasses:
  - Traditional concerns
  - National critical infrastructure protection
    - Including critical private infrastructures
  - Concerns that have not been traditional focus of national security: e.g., currency, privacy, intellectual property
  - Protection of foreign networks and systems upon which we depend
Road Map for National Security:
Imperative for Change

- Serious Gaps Exist in Agencies ability to Protect,
Prevent, and Respond to Terrorist Threats
- A “Catastrophic Attack” is likely to strike the U.S. in the next 25 years
- Need to Reorganize the State and Defense Departments and Invest in Education and Scientific Research
- Create an Independent Cabinet-level National Homeland Security Agency to Coordinate a National Strategy against Terrorism (WMD & Cyber)
US remains economically strong, retains role in shaping int’l environment

S&T advancing at exponential pace, widely but unevenly distributed

World energy, water resources, and global aging become significant factors in the national/global security equations

e-Commerce transcends national boundaries, global interaction in a multitude of markets on a hourly basis 7/24/365.

Asymmetries multiply, threatening US response capabilities

WMDs proliferate to a wider range of state and non-state actors

Conflict will resort to forms and levels of violence shocking to our sensibilities

Alliances and coalitions will be increasingly difficult to establish and sustain

(Excerpted from: Hart-Rudman-Gingrich Commission)
Issues and Observations
• Information Superiority, like information assurance, is dependent on taking a large volume of data, sifting through it to gain key information, leading to knowledge that can be applied as understanding.

• What We Have:

  – Today, the US can gather a vast amount of data through a variety of sources and sensors.
  – Some of that data can be sifted to find the nuggets of key information.
  – A lesser amount is converted to knowledge, and even less is really understood.
Issues in Responding to a Potential Cyber Event

- How do we handle an incident when it is not clear whether it a crime, a foreign attack, or both?
- How should responses be coordinated between National Security and Law Enforcement?
- How should responsibility be handed off once the attacker/criminal is identified?
- How do we interface with the private sector?
Issues (con’t)

- Can a trusted system be composed of untrusted components?
- What role can Active Defense play in Defensive IO?
- Complexity is growing faster than solutions
  - Increased complexity:
    - Makes it more difficult to defend our networked systems
      AND
    - Makes it more difficult for an adversary to predict and evaluate the effects of his attacks
- Defending against information attack is more critical and more difficult than conducting an information attack against an adversary
- From an operational perspective good security often conflicts with getting things done
Conclusions
### Current Status of 1996 DSB Recommendations

<table>
<thead>
<tr>
<th>1996 Recommendation</th>
<th>Pre 9/11 Status</th>
<th>Post 9/11 Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Designate an accountable IW focal point</td>
<td>G</td>
<td>G</td>
</tr>
<tr>
<td>2. Organize for IW-D</td>
<td>Y</td>
<td>YG</td>
</tr>
<tr>
<td>3. Increase awareness</td>
<td>Y</td>
<td>G</td>
</tr>
<tr>
<td>4. Assess infrastructure dependencies and vulnerabilities</td>
<td>R</td>
<td>RY</td>
</tr>
<tr>
<td>5. Define threat conditions and responses</td>
<td>Y</td>
<td>YG</td>
</tr>
<tr>
<td>6. Assess IW-D readiness</td>
<td>R</td>
<td>RY</td>
</tr>
<tr>
<td>7. “Raise the bar” with high-payoff, low-cost items</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>
### Current Status of 1996 DSB Recommendations

<table>
<thead>
<tr>
<th>1996 Recommendation</th>
<th>Pre 9/11 Status</th>
<th>Post 9/11 Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>8. Establish and maintain a minimum essential information infrastructure</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>9. Focus the R&amp;D</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>10. Staff for success</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>11. Resolve the legal issues</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>12. Participate fully in critical infrastructure protection</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>13. Provide the resources</td>
<td>R</td>
<td>Y</td>
</tr>
</tbody>
</table>
### Who Has Responsibility?

<table>
<thead>
<tr>
<th></th>
<th>Cold War</th>
<th>Now</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Assesments</td>
<td>IC</td>
<td>DoD / IC / USG Private Sector</td>
</tr>
<tr>
<td>Indications &amp; Warning</td>
<td>IC</td>
<td>DoD / IC / USG Private Sector</td>
</tr>
<tr>
<td>Attack Characterization &amp; Response</td>
<td>CINCs JCS</td>
<td>DoD / IC / USG Private Sector</td>
</tr>
</tbody>
</table>

A Shared Responsibility
In Some Areas Even 9/11 Did Not Cause Change

- FBI Report – April 2002
  - 90% of businesses and government agencies suffered hacker attacks within the past year.
  - Only 1/3 of those attacks were reported.
  - 80% of those surveyed acknowledged financial losses however, only 44% were willing or able to quantify the damage (~$455M).
  - 78% admitted employee abuse of Internet.
  - 85% had detected viruses on their networks.

- Conclusion: “Now, more than ever, the government and private sector need to work together to share information and be more cognitive of computer security…”
Back-Up Slides
CND Relationships

**National Infrastructure Protection Center (NIPC)**

**Private Sector**
- Information Sharing and Analysis Centers (ISAC)

**Private Sector Critical Industries**
- Telecommunications
- Banking & Finance
- Transportation
- Water Supply
- Energy
- Emergency Services
- Public Health

**DISA**
- National Communications System (NCS)
- National Coordinating Ctr

**Logistic, Technical, Admin Support**

**Tactical Control**
- ARMY (LIWA) ACERT
- AIR FORCE (67 IW) AFCERT
- DISA (GNOSC) DOD CERT
- NAVY (NCTF-CND) NAVCERT
- MARINES (MAR-CND) MIDAS

**Limited Direction**

**Policy Coordination**

**Operational Coordination**

**Intelligence Community**

**Other DoD Agencies**

**Coordination**

**Info Sharing & Advisory Notices**
Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals.

JP 1-02
Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests.

JP 1-02
Electronic Warfare (EW) is any military action involving the use of *electromagnetic* and *directed energy* to control the electromagnetic spectrum or to attack the enemy. The three major subdivisions within Electronic Warfare are:

- **Electronic Warfare (EW)**
- **Electronic Attack (EA)**
- **Electronic Protect (EP)**
- **Electronic Warfare Support (ES)**
OPSEC

OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to:

- Identify those actions that can be observed by adversary intelligence systems
- Determine indicators adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries
- Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation
Physical attack/destruction refers to the use of “hard kill” weapons against designated targets as an element of an integrated IO effort.

Application of combat power to destroy or neutralize enemy forces and installations.

JP 3-13

FM 3-13
CNO – Computer Network Attack Computer Network Defense (CND) and Computer Network Exploitation (CNE) collectively.

DCID 7/3
What Has Changed?

1980
- Monolithic Soviet Threat
- Bi-polar World
- Democracy vs. Communism
- Politics Dominate
- Perimeter / Bastion Concepts
- US Vulnerable Abroad
- Pre-PC Environment
- Peak of the Industrial Age

2002
- US Dominant Global Power
- Europeam Union
- Global Economy
- Economics Dominate
- US Military Budgets
- US Vulnerable at Home
- Computers / Telcom Pervasive
- Dependent on INTERNET
- Rate of Technology Change
- Dawn of the Information Age

We Are Redefining “National Security”
Information Assurance - Current Status

- Architecture: A solid journey is planned, but the roadmap is incomplete.
- Technology: New developments race ahead of understanding (vulnerabilities, dependencies, reliability) -- complexity is growing faster than results.
- People: Limited bench strength.
- R&D: Not using the right seed corn.
- Policy & Legal:
  - Cold War Policy + 19th Century Law ≠ 21st Century Solutions
The Time is Right to Make Progress in Protecting Our Infrastructures

- 8-10 years of experience and study of these issues
- Congress and the Defense Department are sensitized – Particularly since 9-11
- Foreign awareness and programs show substantial growth
- A change in Administration has taken place
- We should lock in and build on key prior recommendations
- Increased private sector involvement